ABSTRACT

A weakly computational zero-knowledge proof class is a relaxed zero-knowledge proof class and is based on a fact that any zero-knowledge proof yields nothing beyond necessary information but a proof system that yields nothing beyond necessary information is not always the zero-knowledge proof. It is ensured that a proof system under a class broader than the zero-knowledge proof class yields nothing beyond necessary information. If it is not included in the zero-knowledge proof class but prevents leakage of information, such a proof system can achieve a higher possibility of designing effective cryptography protocols.